IN THE CLAIMS:

Please cancel claims 8, 15, 18, and 23 without prejudice.

Please amend claims 1, 2, 13, 14, 16, 21, 22, and 24, and add new claims 25-28 as follows:

1. (Currently Amended) A method for secured transfer ~~of an N-byte data element from a first memory containing the data element to a second memory~~ through a data bus that is connected between ~~the~~ a first memory and ~~the~~ a second memory, said method comprising the steps of:

providing an N-byte data element in the first memory;

randomly choosing the value of at least one parameter of a transfer rule before ~~each~~ a transfer of the N-byte data element, the transfer rule defining the order in which the bytes of the N-byte data element are successively transferred through the data bus; and

successively transferring the N bytes of the ~~N-byte~~ data element byte-by-byte through the data bus to the second memory in the order specified by the transfer rule, with each ~~byte~~ of the N bytes transiting once and only once through the data bus.

2. (Currently Amended) The method as defined in claim 1, wherein the transfer rule is a permutation of the bytes of the N-byte data element such that in each transfer of the N-byte data element the N bytes do not successively transit through the data bus ~~is not done~~ in the same byte order.

3. (Original) The method as defined in claim 2, wherein the permutation is defined by the relationship:

$X = (X0 + DIRECTION * PITCH * j)$ modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.

4. (Previously Presented) The method as defined in claim 3, wherein in the step of randomly choosing, the value of PITCH is chosen randomly before each transfer of the data element.

5. (Previously Presented) The method as defined in claim 4, wherein in the step of randomly choosing, the value of DIRECTION is chosen randomly before each transfer of the data element.

6. (Previously Presented) The method as defined in claim 5, wherein in the step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

7. (Previously Presented) The method as defined in claim 3, wherein in the step of randomly choosing, the value of DIRECTION is chosen randomly before each transfer of the data element.

8. (Canceled)

9. (Previously Presented) The method as defined in claim 3, wherein in the step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

10. (Previously Presented) The method as defined in claim 3, wherein in the step of randomly choosing, the value of PITCH and the value of X0 are chosen randomly before each transfer of the data element.

11. (Original) The method as defined in claim 3, wherein PITCH and N are mutually prime numbers.

12. (Original) The method as defined in claim 3, wherein N is a prime integer and PITCH is an integer ranging from 1 to N-1.

13. (Currently Amended) The method as defined in claim 3,

wherein the step of randomly choosing includes the sub-steps of:

determining the values of PITCH, DIRECTION, and X0, the value of at least one of PITCH, DIRECTION, and X0 being randomly chosen; and

initializing j and X, and

the successively transferring step includes the sub-step of repeating N times the steps of:

reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index (X);

writing in the second memory the byte that was read from the first memory; and

incrementing j and varying X.

14. (Currently Amended) A machine-readable medium encoded with a program for secured transfer ~~of an N-byte data element from a first memory containing the data element to a second memory~~ through a data bus that is connected between ~~the~~ a first memory and ~~the~~ a second memory, said program containing instructions for performing the steps of:

providing an N-byte data element in the first memory;

randomly choosing the value of at least one parameter of a transfer rule before ~~each~~ a transfer of the N-byte data element, the transfer rule defining the order in which the bytes of the N-byte data element are successively transferred through the data bus; and

successively transferring the N bytes of the ~~N-byte~~ data element byte-by-byte through the data bus to the second memory in the order specified by the transfer rule, with each ~~byte~~ of the N bytes transiting once and only once through the data bus.

15. (Canceled)

16. (Currently Amended) The machine-readable medium as defined in claim ~~15~~ 14, wherein the permutation is defined by the relationship:

X = (X0 + DIRECTION * PITCH * j) modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.

17. (Previously Presented) The machine-readable medium as defined in claim 16, wherein in the step of randomly choosing, the value of PITCH is chosen randomly before each transfer of the data element.

18. (Canceled)

19. (Previously Presented) The machine-readable medium as defined in claim 16, wherein in the step of randomly choosing, the value of X0 is chosen randomly before each transfer of the data element.

20. (Original) The machine-readable medium as defined in claim 16, wherein PITCH and N are mutually prime numbers.

21. (Currently Amended) The machine-readable medium as defined in claim 16, wherein the step of randomly choosing includes the following sub-steps:

determining the values of PITCH, DIRECTION, and X0, the value of at least one of PITCH, DIRECTION, and X0 being randomly chosen; and

initializing j and X, and

the successively transferring step includes the sub-step of repeating N times the steps of:

reading a byte of the data element from the first memory, the place value of the byte read being equal to the current index (X);

writing in the second memory the byte that was read from the first memory; and

incrementing j and varying X.

22. (Currently Amended) A programmable circuit comprising:

a data bus;

a read-only memory containing an N-byte data element to be transferred, the read-only memory being coupled to the data bus;

a writable memory coupled to the data bus;

a control unit coupled to the read-only memory and the writable memory; and

a random number generator coupled to the control unit, the random number generator supplying the value of at least one parameter of a data transfer rule before ~~each~~ a transfer of the N-byte data element from the read-only memory to the writable memory, the data transfer rule defining the order in which the bytes of the N-byte data element are successively transferred through the data bus,

wherein the control unit controls the data bus such that the N bytes of the ~~N-byte~~ data element ~~is~~ are successively transferred byte-by-byte through the data bus to the writeable memory in the order specified by the data transfer rule, with each ~~byte~~ of the N bytes transiting once and only once through the data bus.

23. (Canceled)

24. (Currently Amended) The programmable circuit as defined in claim ~~23~~ 22, wherein the permutation is defined by the relationship:

X = (X0 + DIRECTION * PITCH * j) modulo N,

where PITCH ranges from 0 to N-1, DIRECTION is either 1 or -1, X0 ranges from 0 to N-1, and j varies from 0 to N-1.

25. (New) The method as defined in claim 1, wherein in the successively transferring step, each of the bytes of the data element is transferred through the data bus without changing the order of bits of that byte.

26. (New) The method as defined in claim 1, wherein each byte of the data element has the same bit order in the first memory, while transiting through the data bus, and in the second memory.

27. (New) The method as defined in claim 1, wherein the successively transferring step includes the sub-steps of:

before each successive transfer of one of the bytes of the data element, using the transfer rule to determine a place value of the byte of the N-byte data element to be transferred;

at each successive transfer of one of the bytes of the data element, transferring the byte of the N-byte data element with the place value that was determined by the transfer rule; and

repeating the using and transferring sub-steps N times so as to successively transfer the N bytes of the data element through the data bus.

28. (New) The method as defined in claim 1, wherein the successively transferring step includes the sub-steps of:

first transferring one byte of the N-byte data element whose place value is defined by the transfer rule;

after the first transferring sub-step, transferring another byte of the N-byte data element whose place value is defined by the transfer rule; and

repeating the sub-step of transferring another byte until the N bytes of the data element have been successively transferred through the data bus in the order specified by the transfer rule.